

Homomorphic Hashing for Sparse Coefficient Extraction

Petteri Kaski¹, Mikko Koivisto², and Jesper Nederlof³

¹ Helsinki Institute for Information Technology, Department of Computer Science, Aalto University, Finland. petteri.kaski@aalto.fi. Supported by the Academy of Finland, Grants 252083 and 256287.

² Helsinki Institute for Information Technology, Department of Computer Science University of Helsinki, Finland. mkhkoivi@cs.helsinki.fi Supported by the Academy of Finland, Grant 125637.

³ Utrecht University, Utrecht, The Netherlands. j.nederlof@uu.nl. Supported by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), project: 'Space and Time Efficient Structural Improvements of Dynamic Programming Algorithms'.

Abstract. We study classes of Dynamic Programming (DP) algorithms which, due to their algebraic definitions, are closely related to coefficient extraction methods. DP algorithms can easily be modified to exploit sparseness in the DP table through memorization. Coefficient extraction techniques on the other hand are both space-efficient and parallelisable, but no tools have been available to exploit sparseness. We investigate the systematic use of homomorphic hash functions to combine the best of these methods and obtain improved space-efficient algorithms for problems including LINEAR SAT, SET PARTITION, and SUBSET SUM. Our algorithms run in time proportional to the number of nonzero entries of the last segment of the DP table, which presents a strict improvement over sparse DP. The last property also gives an improved algorithm for CNF SAT with sparse projections.

1 Introduction

Coefficient extraction can be seen as a general method for designing algorithms, recently in particular in the area of exact algorithms for various NP-hard problems [3,4,14,16,18,25] (cf. [9,26] for an introduction to exact algorithms). The approach of the method is the following (see also [15]):

1. Define a variable (the so-called coefficient) whose value (almost) immediately gives the solution of the problem to be solved,
2. Show that the variable can be expressed by a relatively small formula or circuit over a (cleverly chosen) large algebraic object like a ring or field,
3. Show how to perform operations in the algebraic object relatively efficiently.

In a typical application of the method, the first two steps are derived from an existing Dynamic Programming (DP) algorithm, and the third step deploys a carefully selected algebraic isomorphism, such as the discrete Fourier transform to extract the desired solution/coefficient. Algorithms based on coefficient extraction have two key advantages over DP algorithms; namely, they are space-efficient and they parallelise well (see, for example, [16]).

Yet, DP has an advantage if the problem instance is *sparse*. By this we mean that the number of candidate/partial solutions that need to be considered during DP is small, that is, most entries in the DP table are not used at all. In such a case we can readily adjust the DP algorithm to take this into account through *memorization* so that both the running time and space usage become proportional to the number of partial solutions considered. Unfortunately, it is difficult to parallelise or lower the space usage of memorization. Coefficient extraction algorithms relying on interpolation of sparse polynomials [17] improve over memorization by scaling proportionally only to the number of *candidate* solutions, but their space usage is still not satisfactory (see also [26]).

This paper aims at obtaining what is essentially the best of both worlds, by investigating the systematic use of homomorphisms to “hash down” circuit-based coefficient extraction algorithms so that the domain of coefficient extraction – and hence the running time – matches or improves that of memorization-based DP algorithms, while providing space-efficiency and efficient parallelisation. The key idea is to take an existing algebraic circuit for coefficient extraction (over a sparsely populated algebraic domain such as a ring or field), and transform the circuit into a circuit over a smaller domain by a homomorphic hash function, and only then perform the actual coefficient extraction. Because the function is homomorphic, by hashing the values at the input gates and evaluating the circuit, the output evaluates to the hash of the original output value. Because the function is a hash function, the coefficient to be extracted collides with other coefficients only with negligible probability in the smaller domain, and coefficient extraction can be successfully used on the new (hashed-down) circuit. We call this approach *homomorphic hashing*.

Our and previous results

We study sparse DP/coefficient extraction in three domains: (a) the univariate polynomial ring $\mathbb{F}[x]$ in Section 3, (b) the group algebra $\mathbb{F}[\mathbb{Z}_2^n]$ in Section 4 and (c) the Möbius algebra of the subset lattice in Section 5. The subject of sparse DP or coefficient extraction is highly motivated and well-studied [7,8,17,28]. In [17], a sparse polynomial interpolation algorithm using exponential space was already given for (a) and (b); our algorithms improve these domains to polynomial space. In [14] a polynomial-space algorithm for finding a small multilinear monomial in $\mathbb{F}[\mathbb{Z}_2^n]$ was given. In [16] a general study of settings (a) and (b) was initiated, but sparsity was not addressed. Our main technical contribution occurs with (c) and hashing down to the “Solomon algebra” of a poset.

Our methods work for general arithmetic circuits similarly as in [14,16,17], and most of our algorithms work for counting variants as well. But, for concreteness, we will work here with specific decision problems. Although we mainly give improvements for sparse variants of these problems, we feel the results will be useful to deal with the general case as well (as we will see in Section 4).

Subset Sum The SUBSET SUM problem is the following: given a vector $\mathbf{a} = (a_1, \dots, a_n)$ and integer t , determine whether there exists a subset $X \subseteq [n]$

such that $\sum_{e \in X} a_e = t$. It is known to be solvable $\mathcal{O}^*(2^{n/2})$ time and $\mathcal{O}^*(2^{n/4})$ space [12,21], and solving it faster, or even in $\mathcal{O}^*(1.99^n)$ time and polynomial space are interesting open questions [26]. Recently, a polynomial space algorithm using $\mathcal{O}^*(t)$ time was given in [16].

Theorem 1 *An instance (\mathbf{a}, t) of the SUBSET SUM problem can be solved*

- (a) *in $\mathcal{O}^*(S)$ expected time and polynomial space, and*
- (b) *in $\mathcal{O}^*(S^2)$ time and polynomial space,*

where S is the number of distinct sums, i.e. $S = |\{\sum_{e \in X} a_e : X \subseteq [n]\}|$.

Here it should be noted that standard sparse DP gives an $\mathcal{O}^*(S)$ time and space algorithm. Informally stated, our algorithms hash the instances by working modulo randomly chosen prime numbers and applying the algorithm of [16]. While interesting on their own, these results may be useful in resolving the above open questions when combined with other techniques.

Linear Sat The LINEAR SAT problem is defined as follows: given a matrix $\mathbf{A} \in \mathbb{Z}_2^{n \times m}$, vectors $\mathbf{b} \in \mathbb{Z}_2^m$ and $\boldsymbol{\omega} \in \mathbb{N}^n$, and an integer $t = n^{\mathcal{O}(1)}$, determine whether there is there a vector $\mathbf{x} \in \mathbb{Z}_2^n$ such that $\mathbf{x}\mathbf{A} = \mathbf{b}$ and $\boldsymbol{\omega}\mathbf{x}^T \leq t$.

Variants of LINEAR SAT have been studied, perhaps most notably in [11], where approximability was studied. In [2,6] the Fixed Parameter Tractability was studied for parameterizations of various above guarantees. There, it was also quoted from [11] that (a variant of) LINEAR SAT is “as basic as satisfiability”.

It can be observed that using the approach from [12], LINEAR SAT can be solved in $\mathcal{O}(2^{n/2}m)$ time and $\mathcal{O}(2^{n/2}m)$ space. Also, using standard “sparse dynamic programming”, it can be solved in $\mathcal{O}^*(2^{\text{rk}(\mathbf{A})})$ time and $\mathcal{O}^*(2^{\text{rk}(\mathbf{A})})$ space, where $\text{rk}(\mathbf{A})$ is the rank of \mathbf{A} . We obtain the following polynomial-space variants:

Theorem 2 *An instance $(\mathbf{A}, \mathbf{b}, \boldsymbol{\omega}, t)$ of LINEAR SAT can be solved by algorithms with constant one-sided error probability in*

- (a) *$\mathcal{O}^*(2^{\text{rk}(\mathbf{A})})$ time and polynomial space, and*
- (b) *$\mathcal{O}^*(2^{n/2})$ time and polynomial space.*

The first algorithm hashes the input down using a random linear map and afterwards determines the answer using the Walsh-Hadamard transform. The second algorithm uses a Win/Win approach, combining the first algorithm with the fact that an \mathbf{A} with high rank can be solved with a complementary algorithm.

Satisfiability The CNF-SAT problem is defined as follows: given a CNF-formula $\phi = C_1 \wedge C_2 \wedge \dots \wedge C_m$ over n variables, determine whether ϕ is satisfiable. There are many interesting open questions related to this problem, a major one being whether it can be solved in time $\mathcal{O}^*((2 - \epsilon)^n)$ (the ‘Strong Exponential Time Hypothesis’ [13] states this is not possible), and another being whether the

number of satisfying assignments can be counted in time $\mathcal{O}^*((2 - \epsilon)^n)$ for some $\epsilon > 0$ (e.g. [24]).

A *prefix assignment* is an assignment of 0/1 values to the variables v_1, \dots, v_i for some $1 \leq i \leq n$. A *projection* (*prefix projection*) of a CNF-formula is a subset $\pi \subseteq [m]$ such that there exists an assignment (prefix assignment) of the variables such that for every $1 \leq j \leq m$ it satisfies C_j if and only if $j \in \pi$. An algorithm for CNF-SAT running in time linear in the number of *prefix* projections can be obtained by standard sparse DP. However, it is sensible to ask about complexity of CNF-SAT if the number of projections is small. We give a positive answer:

Theorem 3 *Satisfiability of a formula $\phi = C_1 \wedge \dots \wedge C_m$ can be determined in $\mathcal{O}^*(P^2)$ time and $\mathcal{O}^*(P)$ space, where $P = |\{\pi \subseteq [m] : \pi \text{ is a projection of } \phi\}|$.*

We are not aware of previous work that studies instances with few projections. Although most instances will have many projections, we think our result opens up a fresh technical perspective that may contribute towards solving the above mentioned and related questions.

Underlying Theorem 3 is our main technical contribution (Theorem 16) that enables us to circumvent partial projections and access projections directly, namely homomorphic hashing from the Möbius algebra of the lattice of subsets of $[m]$ to the Solomon algebra of a poset. A full proof of Theorem 16 is given in the appendix; we give a specialized, more direct proof of Theorem 3 in Section 5.

The proofs of claims marked with a “†” are relegated to the appendix in order to not break the flow of the paper.

2 Notation and Preliminaries

Lower-case boldface characters refer to vectors, while capital boldface letters refer to matrices, \mathbf{I} being the identity matrix. The rank of a matrix \mathbf{A} is denoted by $\text{rk}(\mathbf{A})$. If R and S are sets, and S is finite, denote by R^S the set of all $|S|$ -dimensional vectors with values in R , indexed by elements of S , that is, if $\mathbf{v} \in R^S$, then for every $e \in S$ we have $v_e \in R$. We denote by \mathbb{Z} and \mathbb{N} the set of integers and non-negative integers, respectively, and by \mathbb{Z}_p the field of integers modulo a prime p . An arbitrary field is denoted by \mathbb{F} .

For a logical proposition P , we use Iverson’s bracket notation $[P]$ to denote a 1 if P is true and a 0 if P is false. For a function $h : A \rightarrow B$ and $b \in B$, the preimage $h^{-1}(b)$ is defined as the set $\{a \in A : h(a) = b\}$. For an integer n and $A \subseteq \{1, \dots, n\}$, denote by $\chi(A) \in \mathbb{Z}_2^n$ the characteristic vector of A . Sometimes we will state running times of algorithms with the \mathcal{O}^* notation, which suppresses any factor polynomial in the input size.

For a ring R and a finite set S , we write R^S for the ring consisting of the set R^S (the set of all vectors over R with coordinates indexed by elements of S) equipped with coordinate-wise addition $+$ and multiplication \circ (the *Hadamard product*), that is, for $\mathbf{a}, \mathbf{b} \in R^S$ and $\mathbf{a} + \mathbf{b} = \mathbf{c}$, $\mathbf{a} \circ \mathbf{b} = \mathbf{d}$ we set $a_z + b_z = c_z$ and $a_z b_z = d_z$ for each $z \in S$, where $+$ and the juxtaposition denote addition

and multiplication in R , respectively. The inner-product $\mathbf{a}, \mathbf{b} \in R^S$ is denoted by $\mathbf{a}^T \cdot \mathbf{b}$. For $\mathbf{v} \in R^S$ denote by $\text{supp}(\mathbf{v}) \subseteq S$ the *support* of \mathbf{v} , that is, $\text{supp}(\mathbf{v}) = \{z \in S : v_z \neq 0\}$, where 0 is the additive identity element of R . A vector \mathbf{v} is called a *singleton* if $|\text{supp}(\mathbf{v})| = 1$. We denote by $\langle w, z \rangle$ the singleton with value w on index z , that is, $\langle w, z \rangle_y = w[y = z]$ for all $y \in S$.

If R is a ring and (S, \cdot) is a finite semigroup, denote by $R[S]$ the ring consisting of the set R^S equipped with coordinate-wise addition and multiplication defined by the convolution operator $*$, where for $\mathbf{a}, \mathbf{b} \in R^S$, $\mathbf{a} * \mathbf{b} = \mathbf{c}$ we set $c_z = \sum_{x \cdot y = z} a_x b_y$ for every $z \in S$.

If R, S are rings with operations $(+, *)$ and (\oplus, \otimes) respectively, a *homomorphism from R to S* is a function $h : R \rightarrow S$ such that $h(e_1 + e_2) = h(e_1) \oplus h(e_2)$ and $h(e_1 * e_2) = h(e_1) \otimes h(e_2)$ for every $e_1, e_2 \in R$.

Observation 4 *Let R be a ring, and let (S, \cdot) and (T, \odot) be finite semigroups. Suppose $\varphi : S \rightarrow T$ such that for every $x, y \in S$ we have $\varphi(x \cdot y) = \varphi(x) \odot \varphi(y)$. Then the function $h : R[S] \rightarrow R[T]$ defined by $h : \mathbf{a} \mapsto \mathbf{b}$ where $b_z = \sum_{y \in \varphi^{-1}(z)} a_y$ for all $z \in T$ is a homomorphism.*

A *circuit C* over a ring R is a labeled directed acyclic graph $D = (V, A)$ where the elements of V are called *gates* and D has a unique sink called the *output gate* of C . All sources of C are called *input gates* and are labeled with elements from R . All gates with non-zero in-degree are labeled as either an *addition* or a *multiplication gate*. (If multiplication in R is not commutative, the in-arcs of each multiplication gate are also ordered.) Every gate g of C can be associated with a ring element in the following natural way: If g is an input gate, we associate the label of g with g . If g is an addition gate we associate the ring element $e_1 + \dots + e_d$ with g , and if g is a multiplication gate we associate the ring element $e_1 * \dots * e_d$ with g where e_1, \dots, e_d are the ring elements associated with the d in-neighbors of g , and $+$ and $*$ are the operations of the ring R .

Suppose the ground set of R is of the type A^B where A, B are sets. Then C is said to have *singleton inputs* if the label of every input-gate of C is a singleton vector of R .

Definition 5 *Let R and S be rings, let $h : R \rightarrow S$ be a homomorphism, and suppose that C is a circuit over R . Then, the circuit $h(C)$ over S obtained by applying h to C is defined as the circuit obtained from C by replacing for every input gate the label l by $h(l)$.*

Note that the following is immediate from the definition of a homomorphism:

Observation 6 *Suppose C is a circuit over a ring R with output $v \in R$. Then the circuit over S obtained by applying a homomorphism $h : R \rightarrow S$ to C outputs $h(v) \in S$.*

3 Homomorphic Hashing for Subset Sum

In this section we will study the SUBSET SUM problem and prove Theorem 1. As mentioned in the introduction, it should be noted that this merely serves as an

illustration of how similar problems can be tackled as well since the same method applies to the more general sparse polynomial interpolation problem. However, to avoid a repeat of the analysis of [16], we have chosen to restrict ourselves to the SUBSET SUM problem. Our central contribution over [16] is that we take advantage of sparsity.

Given $\mathbf{a} \in \mathbb{N}^n$ and an integer $p \in \mathbb{N}$, let $c^p : \mathbb{N}^n \rightarrow \mathbb{N}^n$ be defined by

$$c^p(\mathbf{a})_j = \left| \left\{ X \subseteq [n] : \sum_{e \in X} a_e \equiv j \pmod{p} \right\} \right| \text{ for every } j \in \mathbb{Z}_p.$$

We also use the shorthand $\mathbf{c}(\mathbf{a}) = \mathbf{c}^\infty(\mathbf{a})$. We use a corollary from [16]:

Corollary 7 (\dagger , [16]) *Given an instance (\mathbf{a}, t) of SUBSET SUM and an integer p , $c^p(\mathbf{a})_t$ can be computed in $\mathcal{O}^*(p)$ time and $\mathcal{O}^*(1)$ space.*

We will also need the following two results on primes:

Theorem 8 ([20]) *If $55 < u$, then the number of prime numbers at most u is at least $\frac{u}{\ln u + 2}$.*

Lemma 9 (\dagger , Folklore) *There exists an algorithm `pickprime`(u) running in $\text{polylog}(u)$ time that, given integer $u \geq 2$ as input, outputs either a prime chosen uniformly at random from the set of primes at most u or `notfound`. Moreover, the probability that the output is `notfound` is at most $\frac{1}{e}$.*

We will run a data reduction procedure similar to the one of Claim 2.7 in [10], before applying the algorithm of Corollary 7. The idea of the data reduction procedure is to work modulo a prime of size roughly $|\text{supp}(\mathbf{c}(\mathbf{a}))|$ or larger:

Lemma 10 *Let $S \geq |\text{supp}(\mathbf{c}(\mathbf{a}))|$ and let β be an upper bound on the number of bits needed to represent the integers, i.e. $2^\beta > \max\{t, \max_i a_i\}$. Then, $\text{Prob}_p[\mathbf{c}(\mathbf{a})_t = c^p(\mathbf{a})_t] \geq \frac{1}{2}$, where the probability is taken uniformly over all primes $p \leq S\beta n(\log \beta)(\log n)$.*

Proof. Suppose $\mathbf{c}(\mathbf{a})_t \neq c^p(\mathbf{a})_t$. Then there exists an integer $u \in \text{supp}(\mathbf{c}(\mathbf{a}))$ such that $u \neq t$ and $u \equiv t \pmod{p}$. This implies that p is a divisor of $|t - u|$, so let us bound the probability of this event. Since $|t - u| \leq 2^\beta n$, it has at most $\beta + \log n$ distinct prime divisors. Let $\gamma = S\beta n(\log \beta)(\log n)$. It is easy to check that for sufficiently large β and n :

$$\text{Prob}_p[p \text{ divides } |t - u|] \leq \frac{\beta + \log n}{\frac{\gamma}{\log \gamma + 2}} \leq \frac{\beta + \log n}{\frac{\gamma}{3(n + \log \beta)}} \leq \frac{1}{2S},$$

where we use Theorem 8 in the first inequality and $S \leq 2^n$ in the second inequality. Applying the union bound over the at most S elements of $\text{supp}(\mathbf{c}(\mathbf{a}))$, the event that there exists a $u \in \text{supp}(\mathbf{c}(\mathbf{a}))$ with $u \neq t$ and $u \equiv t \pmod{p}$ has probability at most $\frac{1}{2}$. \square

Now we give two algorithms utilizing homomorphic hashing, one for the case where S is known, and one for the case where S is not known.

Theorem 11 *There exists an algorithm that, given an instance (\mathbf{a}, t) of the SUBSET SUM problem and an integer $S \geq |\text{supp}(c(\mathbf{a}))|$ as input, outputs a non-negative integer x in $\mathcal{O}^*(S)$ time and polynomial space such that (i) $x = 0$ implies $c(\mathbf{a})_t = 0$ and (ii) $\text{Prob}[c(\mathbf{a})_t = x] \geq \frac{1}{4}$.*

Proof. The algorithm is: First, obtain prime $p = \text{pickprime}(S\beta n(\log \beta)(\log n))$ using Lemma 9. Second, compute and output $c^p(\mathbf{a})_t$ using Corollary 7. Condition (i) holds since $c^p(\mathbf{a})_t = 0$ implies $c(\mathbf{a})_t = 0$ for any p, t . Moreover, condition (ii) follows from Lemma 10 and Lemma 9 since $\frac{1}{2}(1 - \frac{1}{e}) \geq \frac{1}{4}$. The time and space bounds are met by Corollary 7 because $p = \mathcal{O}^*(S)$. \square

Proof (of Theorem 1(a)). The algorithm is the following: Maintain a guess S of $\text{supp}(c(\mathbf{a}))$, initially set to n . Obtain a prime $p = \text{pickprime}(S\beta n(\log \beta)(\log n))$ using Lemma 9, and compute $c^p(\mathbf{a})_t$ using Corollary 7. If $c^p(\mathbf{a})_t = 0$ output **no** since $c(\mathbf{a})_t = 0$; otherwise, attempt to construct a subset $X \subseteq [n]$ such that $\sum_{e \in X} a_e = t$ using self-reduction. If this succeeds, return **yes**. Otherwise, double S and repeat. The expected running time (taken over all primes p) is $\mathcal{O}^*(\text{supp}(c(\mathbf{a})))$ because when $S \geq \text{supp}(c(\mathbf{a}))\beta n(\log \beta)(\log n)$ the probability of successfully constructing a solution or concluding that none exist is at least $\frac{1}{2}$ by the arguments in the proof of Lemma 10. \square

The derandomization for Theorem 1(b) is given in the appendix.

4 Homomorphic Hashing for Linear Satisfiability

In this section we assume that \mathbb{F} is a field of non-even characteristic and that addition and multiplication refer to operations in \mathbb{F} . For $s \in \mathbb{N}$, we denote by $\Phi \in \mathbb{F}^{\mathbb{Z}_2^s \times \mathbb{Z}_2^s}$ the *Walsh-Hadamard matrix*, defined for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^s$ by $\Phi_{\mathbf{x}, \mathbf{y}} = (-1)^{\mathbf{x}\mathbf{y}^T}$.

Lemma 12 (Folklore) *The Walsh-Hadamard matrix satisfies $\Phi\Phi = 2^s \mathbf{I}$ and, for every $\mathbf{f}, \mathbf{g} \in \mathbb{F}[\mathbb{Z}_2^s]$, it holds that $(\mathbf{f} * \mathbf{g})\Phi = \mathbf{f}\Phi \circ \mathbf{g}\Phi$.*

We first prove the following general theorem, of which Theorem 2(a) is a special case.

Theorem 13 *There exists a randomized algorithm that, given as input*

1. *a circuit C with singleton inputs over $\mathbb{F}[\mathbb{Z}_2^n]$,*
2. *an integer $S \geq |\text{supp}(\mathbf{v})|$, and*
3. *an element $\mathbf{t} \in \mathbb{Z}_2^n$,*

outputs the coefficient $v_{\mathbf{t}} \in \mathbb{F}$ with probability at least $\frac{1}{2}$, where $\mathbf{v} \in \mathbb{F}[\mathbb{Z}_2^n]$ is the output of C . The algorithm runs in time $\mathcal{O}^(S)$ and uses $\mathcal{O}^*(S)$ arithmetic operations in \mathbb{F} , and requires storage for $\mathcal{O}^*(1)$ bits and elements of \mathbb{F} .*

Algorithm hashZ2

- 1: Let $s = \lceil \log S \rceil + 1$.
- 2: Choose a matrix $\mathbf{H} \in \mathbb{Z}_2^{s \times n}$ uniformly at random from the set of all $s \times n$ matrices with binary entries.
- 3: Let $h : \mathbb{F}[\mathbb{Z}_2^n] \rightarrow \mathbb{F}[\mathbb{Z}_2^s]$ be the homomorphism defined by $h(\mathbf{a}) = \mathbf{b}$ where $b_x = \sum_{\mathbf{y} \in \mathbb{Z}_2^n : \mathbf{yH} = \mathbf{x}} a_{\mathbf{y}}$ for all $\mathbf{x} \in \mathbb{Z}_2^s$. Apply h to C to obtain the circuit C_1 .
- 4: **return** $\frac{1}{2^s} \sum_{\mathbf{x} \in \mathbb{Z}_2^s} (-1)^{(\mathbf{tH})\mathbf{x}^T} \text{sub}(C_1, \mathbf{x})$.

Algorithm sub(C_1, \mathbf{x})

- 5: Let $\varphi : \mathbb{F}[\mathbb{Z}_2^s] \rightarrow \mathbb{F}$ be the homomorphism defined by $\varphi(\mathbf{w}) = \sum_{\mathbf{y} \in \mathbb{Z}_2^s} (-1)^{\mathbf{x}\mathbf{y}^T} w_{\mathbf{y}}$ for all $\mathbf{w} \in \mathbb{F}[\mathbb{Z}_2^s]$. Apply φ to C_1 to obtain the circuit C_2 .
- 6: Evaluate C_2 and return the output.

Algorithm 1: Homomorphic hashing for Theorem 13.

Proof. The algorithm is given in Algorithm 1. Let us first analyse the complexity of this algorithm: Steps 1 and 2 can be performed in time polynomial in the input. Step 3 also be done in polynomial time since it amounts to relabeling all input gates with $h(\mathbf{e})$ where \mathbf{e} was the old label. Indeed, we know that $\mathbf{e} \in \mathbb{F}[\mathbb{Z}_2^n]$ is a singleton $\langle v, \mathbf{y} \rangle$, so $h(\mathbf{e})$ is the singleton $\langle v, \mathbf{yH} \rangle$ and this can be computed in polynomial time. Step 4 takes $\mathcal{O}^*(S)$ operations and calls to **sub**, so for the complexity bound it remains to show that each call to **sub** runs in polynomial time. Step 5 can be implemented in polynomial time similar to Step 3 since the singleton $\mathbf{e} = \langle v, \mathbf{y} \rangle$ is mapped to $(-1)^{\mathbf{x}\mathbf{y}^T} v$. Finally, the direct evaluation of C_2 uses $|C_2|$ operations in \mathbb{F} . Hence the algorithm meets the time bound, and also the space bound is immediate.

The fact that **hashZ2** returns $v_{\mathbf{t}}$ with probability at least $\frac{1}{2}$ is a direct consequence of the following two claims. Let \mathbf{w} be the output of C_1 .

Claim 1 (†) $\text{Prob}_{\mathbf{H}}[v_{\mathbf{t}} = w_{\mathbf{tH}}] \geq \frac{1}{2}$.

Claim 2 (†) *Algorithm hashZ2 returns $w_{\mathbf{tH}}$.*

□

Proof (of Theorem 2(a)). For $1 \leq i \leq n$ and $0 \leq w \leq t$ denote by $\mathbf{A}^{(i)}$ the i th row of \mathbf{A} and define $\mathbf{f}[i, w] \in \mathbb{Q}[\mathbb{Z}_2^m]$ by

$$\mathbf{f}[i, w] = \begin{cases} \langle 1, \mathbf{0} \rangle & \text{if } i = w = 0, \\ 0 & \text{if } i = 0 \text{ and } w \neq 0, \\ \mathbf{f}[i-1, w] + \mathbf{f}[i-1, j - \omega_i] * \langle 1, \mathbf{A}^{(i)} \rangle & \text{otherwise.} \end{cases} \quad (1)$$

It is easy to see that for every $1 \leq i \leq n$, $0 \leq w \leq t$, and $\mathbf{y} \in \mathbb{Z}_2^m$, the value $\mathbf{f}[i, w]_{\mathbf{y}}$ is the number of $\mathbf{x} \in \mathbb{Z}_2^i$ such that $\tilde{\omega}\mathbf{x}^T = t$ and $\mathbf{x}\tilde{\mathbf{A}} = \mathbf{y}$ where $\tilde{\omega}$ and $\tilde{\mathbf{A}}$ are obtained by truncating ω and \mathbf{A} to the first i rows. Hence, we let C be

the circuit implementing 1 and let its output be $\mathbf{v} = \sum_{w=0}^t \mathbf{f}[n, w]$. Thus, $v_{\mathbf{b}}$ is the number of $\mathbf{x} \in \mathbb{Z}_2^n$ with $\mathbf{x}\mathbf{A} = \mathbf{b}$ and $\mathbf{x}\boldsymbol{\omega}^T \leq t$.

Also, $|\text{supp}(\mathbf{v})| \leq 2^{\text{rk}(\mathbf{A})}$ since any element of the support of \mathbf{v} is a sum of rows of \mathbf{A} and hence in the row-space of \mathbf{A} , which has size at most $2^{\text{rk}(\mathbf{A})}$. To apply Theorem 13, let $\mathbb{F} = \mathbb{Q}$ and observe that the computations are in fact carried out over integers bounded in absolute value poly-exponentially in n and hence the operations in the base field can also be executed polynomial in n . The theorem follows from Theorem 13. \square

To establish Theorem 2(b), let us first see how to exploit a high linear rank of the matrix \mathbf{A} in an instance of LINEAR SAT. By permuting the rows of \mathbf{A} as necessary, we can assume that the first $\text{rk}(\mathbf{A})$ rows of \mathbf{A} are linearly independent. We can now partition \mathbf{x} into $\mathbf{x} = (\mathbf{y}, \mathbf{z})$, where \mathbf{y} has length $\text{rk}(\mathbf{A})$ and \mathbf{z} has length $n - \text{rk}(\mathbf{A})$. There are $2^{n - \text{rk}(\mathbf{A})}$ choices for \mathbf{z} , each of which by linear independence has at most one corresponding \mathbf{y} such that $\mathbf{x}\mathbf{A} = \mathbf{b}$. Given \mathbf{z} , we can determine the corresponding \mathbf{y} (if any) in polynomial time by Gaussian elimination. Thus, we have:

Observation 14 LINEAR SAT can be solved in $\mathcal{O}^*(2^{n - \text{rk}(\mathbf{A})})$ time and polynomial space.

This enables a “Win/Win approach” where we distinguish between low and high ranks, and use an appropriate algorithm in each case.

Proof (of Theorem 2(b)). Compute $\text{rk}(\mathbf{A})$. If $\text{rk}(\mathbf{A}) \geq n/2$, run the algorithm of Observation 14. Otherwise, run the algorithm implied by Theorem 2(a). \square

Set Partition We now give a very similar application to the SET PARTITION problem: given an integer t and a set family $\mathcal{F} \subseteq 2^U$ where $|\mathcal{F}| = n$, $|U| = m$, determine whether there is a subfamily $\mathcal{P} \subseteq \mathcal{F}$ with $|\mathcal{P}| \leq t$ such that $\bigcup_{S \in \mathcal{P}} S = U$ and $\sum_{S \in \mathcal{P}} |S| = |U|$.

The *incidence matrix* of a set system (U, \mathcal{F}) is the $|U| \times |\mathcal{F}|$ matrix \mathbf{A} whose entries $A_{e,S} = [e \in S]$ are indexed by $e \in U$ and $S \in \mathcal{F}$.

Theorem 15 (†) *There exist algorithms that given an instance (U, \mathcal{F}, t) of SET PARTITION output the number of set partitions of size at most t with probability at least $\frac{1}{2}$, and use (a) $\mathcal{O}^*(2^{\text{rk}(\mathbf{A})})$ time and polynomial space, and (b) $(2^{\text{rk}(\mathbf{A})} + n)m^{\mathcal{O}(1)}$ time and space, where \mathbf{A} is the incidence matrix of (U, \mathcal{F}) .*

5 Homomorphic Hashing for the Union Product

In this section our objective is to mimic the approach of the previous section for $\mathbb{N}[(2^U, \cup)]$, where $(2^U, \cup)$ is the semigroup defined by the set union \cup operation on 2^U , the power set of an n -element set U . The direct attempt to apply a homomorphic hashing function, unfortunately, fails. Indeed, let h be an arbitrary homomorphism from $(2^U, \cup)$ to $(2^V, \cup)$ with $|V| < |U|$. Let $U = \{e_1, e_2, \dots, e_n\}$ and consider the minimum value $1 \leq j \leq n - 1$ with

$h(\{e_1, \dots, e_j\}) = \cup_{i=1}^j h(\{e_i\}) = \cup_{i=1}^{j+1} h(\{e_i\}) = h(\{e_1, \dots, e_{j+1}\})$; in particular, for $X = \{e_1, \dots, e_j, e_{j+2}, \dots, e_n\} \neq U$ we have $h(X) = h(U)$, which signals failure since we cannot isolate X from U .

Instead, we use hashing to an algebraic structure based on a poset (the “Solomon algebra” of a poset due to [22]) that is obtained by the technique “Iterative Compression”. This gives the following main result. For reasons of space we relegate a detailed proof to the appendix; here we will give a simplified version of the proof in the special case of Theorem 3 in this section.

Theorem 16 (†) *Let and $|U| = n$. There are algorithms that, given a circuit C with singleton inputs in $\mathbb{N}[(2^U, \cup)]$ outputting \mathbf{v} , compute*

- (a) *a list with v_X for every $X \in \text{supp}(\mathbf{v})$ in $\mathcal{O}^*(|\text{supp}(\mathbf{v})|^2 \cdot n^{\mathcal{O}(1)})$ time,*
- (b) *v_U in time $\mathcal{O}^*(2^{(1-\alpha/2)n} n^{\mathcal{O}(1)})$ if $0 < \alpha \leq 1/2$ such that $|\text{supp}(\mathbf{v})| \leq 2^{(1-\alpha)n}$.*

The above result is stated for simplicity in the unit-cost model, that is, we assume that arithmetic operations on integers take constant time. For the more realistic log-cost model, where such operations are assumed to take time polynomial in the number of bits of the binary representation, we only mention here that our results also hold under some mild technical conditions. Let us first show that Theorem 3(a) indeed is a special case of Theorem 16:

Proof (of Theorem 3). Use a circuit over $\mathbb{N}[(2^{[m]}, \cup)]$ that implements the expression

$$\mathbf{f} = (\langle 1, V_1 \rangle + \langle 1, \bar{V}_1 \rangle) * (\langle 1, V_2 \rangle + \langle 1, \bar{V}_2 \rangle) * \dots * (\langle 1, V_m \rangle + \langle 1, \bar{V}_m \rangle),$$

where $V_i \subseteq [m]$ (respectively, $\bar{V}_i \subseteq [m]$) is the set of all indices of clauses that contain a positive (respectively, negative) literal of the variable v_i . Then use Theorem 16 to determine $f_{[m]}$, the number of satisfying assignments of ϕ . \square

Now we proceed with a self-contained proof Theorem 3. Given poset (P, \leq) , the *Möbius function* $\mu : P \times P \rightarrow \mathbb{N}$ of P is defined for all $x, y \in P$ by

$$\mu(x, y) = \begin{cases} 1 & \text{if } x = y, \\ -\sum_{x \leq y < z} \mu(y, z) & \text{if } x < z, \\ 0 & \text{otherwise.} \end{cases} \quad (2)$$

The *zeta transform* ζ and *Möbius transform* μ are the $|P| \times |P|$ matrices defined by $\zeta_{x,y} = [x \leq y]$ and $\mu_{x,y} = \mu(x, y)$ for all $x, y \in P$. For a CNF-formula ϕ denote $\text{supp}(\phi)$ for the set of all projections of ϕ . Recall in Theorem 3 we are given a CNF-Formula $\phi = C^1 \wedge \dots \wedge C^m$ over n variables. For $i = 1, \dots, m$ define $\phi_i = C^1 \wedge \dots \wedge C^i$. Then we have the following easy observations

1. $\text{supp}(\phi_0) = \{\emptyset\}$,
2. $\text{supp}(\phi_i) \subseteq \text{supp}(\phi_{i-1}) \cup \{X \cup \{i\} : X \in \text{supp}(\phi_{i-1})\}$ for every $i = 1, \dots, m$,
3. $|\text{supp}(\phi_{i-1})| \leq |\text{supp}(\phi_i)|$ for every $i = 1, \dots, m$.

Given the above lemma and observations, we will give an algorithm using a technique called *iterative compression* [19]. As we will see, by this technique it is sufficient to solve the following “compression problem”:

Lemma 17 *Given a CNF-formula $\phi = C_1 \wedge \dots \wedge C_m$ and a set family $\mathcal{F} \subseteq 2^{[m]}$ with $\text{supp}(\phi) \subseteq \mathcal{F}$, the set $\text{supp}(\phi)$ can be constructed in $\mathcal{O}^*(|\mathcal{F}|^2)$ time.*

Proof. In what follows $\mathbf{a} \in \{0, 1\}^n$ refers to an assignment of values to the n variables in ϕ . Define $\mathbf{f} \in \mathbb{N}^{2^{[m]}}$ for all $X \subseteq [m]$ by

$$f_X = |\{\mathbf{a} \in \{0, 1\}^n : \forall i \in [m] \text{ it holds that } \mathbf{a} \text{ satisfies } C_i \text{ iff } i \in X\}|.$$

It is easy to see that $\text{supp}(\mathbf{f}) = \text{supp}(\phi)$, so if we know f_X for every $X \in \mathcal{F}$ we can construct $\text{supp}(\phi)$ in $|\mathcal{F}|$ time. Towards this end, first note that for every $Y \subseteq [m]$ it holds that

$$\begin{aligned} (\mathbf{f}\zeta)_Y &= \sum_{\substack{X \in \text{supp}(\mathbf{f}) \\ X \subseteq Y}} f(X) = \sum_{X \subseteq Y} f(X) \\ &= |\{\mathbf{a} \in \{0, 1\}^n : \forall i \in [m] \text{ it holds that } \mathbf{a} \text{ satisfies } C_i \text{ only if } i \in Y\}|. \end{aligned}$$

Second, note that the last quantity can be computed in polynomial time: since every clause outside Y must not be satisfied, each such clause forces the variables that occur in it to unique values; any other variables may be assigned to arbitrary values. That is, the count is 0 if the clauses outside Y force at least one variable to conflicting values, otherwise the count is 2^a where a is the number of variables that occur in none of the clauses outside Y .

Now the algorithm is the following: for every $X \in \mathcal{F}$ compute $(\mathbf{f}\zeta)_X$ in polynomial time as discussed above. Then we can use algorithm **mobius** as described below to obtain f_X for every $X \in \mathcal{F}$ since it follows that $\mathbf{f} = \text{mobius}((\mathcal{F}, \subseteq), \mathbf{f}\zeta)$ from the definition of μ and the fact that $\mu\zeta = \mathbf{I}$. Algorithm **mobius** clearly runs in $\mathcal{O}^*(|P|^2)$ time, so this procedure meets the claimed time bound.

Algorithm mobius $((P, \leq), \mathbf{w})$

- 1: Let $P = \{v_1, v_2, \dots, v_{|P|}\}$ such that $v_i \leq v_j$ implies $i \geq j$.
- 2: $\mathbf{z} \leftarrow \mathbf{w}$.
- 3: **for** $i = 1, 2, \dots, |P|$ **do**
- 4: **for every** $v_j \leq v_i$ **do**
- 5: $z_i = z_i - z_j$
- 6: **return** \mathbf{z} .

□

Proof (of Theorem 3, self-contained). Recall that we already know that $\text{supp}(\phi_0) = \{\emptyset\}$. Now, for $i = 1, \dots, m$ we set $\mathcal{F} = \text{supp}(\phi_{i-1}) \cup \{X \cup \{i\} : X \in \text{supp}(\phi_{i-1})\}$ and use \mathcal{F} to obtain $\text{supp}(\phi_{i-1})$ using Lemma 17. In the end we are given $\text{supp}(\phi_m)$ and since ϕ_m is exactly the original formula, the input is a yes-instance if and only if $[m] \in \text{supp}(\phi_m)$. The claimed running time follows from Observations 1 and 3 above and the running time of algorithm **mobius**. □

Set Cover We will now give an application of Theorem 16(b) to SET COVER: Given a set family $\mathcal{F} \subseteq 2^U$ where $|U| = n$ and an integer k , find a subfamily $\mathcal{C} \subseteq \mathcal{F}$ such that $|\mathcal{C}| = k$ and $\bigcup_{S \in \mathcal{C}} S = U$.

Theorem 18 *Given an instance of SET COVER, let $0 < \alpha \leq 1/2$ be the largest real such that $|\{\bigcup_{S \in \mathcal{C}} S : \mathcal{C} \subseteq \mathcal{F} \wedge |\mathcal{C}| = k\}| \leq 2^{(1-\alpha)n}$. Then the instance can be solved in $\mathcal{O}^*(2^{(1-\alpha/2)n} n^{\mathcal{O}(1)})$ time (and exponential space).*

Proof. Let $\mathcal{F} = \{S_1, \dots, S_m\}$, and for every $1 \leq i \leq m$ and $1 \leq j \leq n$ define $f[i, j]$ as follows:

$$f[i, j] = \begin{cases} \langle 1, \emptyset \rangle & \text{if } i = j = 0, \\ f[i-1, j] + f[i-1, j-1] * \langle 1, S_i \rangle & \text{otherwise.} \end{cases}$$

It is easy to see that for every $X \subseteq U$ we have that $f[i, j]_X$ is the number of $\mathcal{C} \subseteq \{S_1, \dots, S_i\}$ such that $|\mathcal{C}| = j$ and $\bigcup_{S \in \mathcal{C}} S = X$. Hence the theorem follows directly by applying Theorem 16(b) by interpreting the above recurrence as a circuit in order to determine the value $f[m, k]_U$. \square

References

1. M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2):781–793, 2004.
2. N. Alon, G. Gutin, E. J. Kim, S. Szeider, and A. Yeo. Solving MAX- r -SAT above a tight lower bound. *Algorithmica*, 61(3):638–655, 2011.
3. A. Björklund. Determinant sums for undirected Hamiltonicity. In *FOCS*, pages 173–182. IEEE Computer Society, 2010.
4. A. Björklund, T. Husfeldt, and M. Koivisto. Set partitioning via inclusion-exclusion. *SIAM J. Comput.*, 39(2):546–563, 2009.
5. R. S. Boyer and J. S. Moore. Mjrtty: A fast majority vote algorithm. In *Automated Reasoning: Essays in Honor of Woody Bledsoe*, pages 105–118, 1991.
6. R. Crowston, G. Gutin, M. Jones, and A. Yeo. Lower bound for Max- r -Lin2 and its applications in algorithmics and graph theory. *CoRR*, abs/1104.1135, 2011.
7. D. Eppstein, Z. Galil, R. Giancarlo, and G. F. Italiano. Sparse dynamic programming I: linear cost functions. *J. ACM*, 39:519–545, 1992.
8. D. Eppstein, Z. Galil, R. Giancarlo, and G. F. Italiano. Sparse dynamic programming II: convex and concave cost functions. *J. ACM*, 39(3):546–567, 1992.
9. F. V. Fomin and D. Kratsch. *Exact Exponential Algorithms*. Springer-Verlag New York, Inc., New York, NY, USA, 1st edition, 2010.
10. D. Harnik and M. Naor. On the compressibility of NP instances and cryptographic applications. *SIAM Journal on Computing*, 39(5):1667–1713, 2010.
11. J. Håstad. Some optimal inapproximability results. *J. ACM*, 48:798–859, 2001.
12. E. Horowitz and S. Sahni. Computing partitions with applications to the knapsack problem. *J. ACM*, 21:277–292, 1974.
13. R. Impagliazzo and R. Paturi. On the complexity of k -SAT. *J. Comput. Syst. Sci.*, 62(2):367–375, 2001.
14. I. Koutis and R. Williams. Limits and applications of group algebras for parameterized problems. In *ICALP 2009*.

15. R. J. Lipton. Beating Bellman for the knapsack problem. 2010, <http://rjlipton.wordpress.com>.
16. D. Lokshtanov and J. Nederlof. Saving space by algebraization. In *Proceedings of the 42nd ACM Symposium on Theory of Computing*, STOC'10, pages 321–330, New York, 2010. ACM.
17. Y. Mansour. Randomized interpolation and approximation of sparse polynomials. *SIAM J. Comput.*, 24(2):357–368, 1995.
18. J. Nederlof. Fast polynomial-space algorithms using Möbius inversion: Improving on Steiner tree and related problems. In *ICALP 2009*.
19. B. A. Reed, K. Smith, and A. Vetta. Finding odd cycle transversals. *Oper. Res. Lett.*, 32(4):299–301, 2004.
20. B. Rosser. Explicit bounds for some functions of prime numbers. *American Journal of Mathematics*, 63(1):211–232, 1941.
21. R. Schroeppel and A. Shamir. A $T = O(2^{n/2})$, $S = O(2^{n/4})$ algorithm for certain NP-complete problems. *SIAM J. Comput.*, 10(3):456–464, 1981.
22. L. Solomon. The burnside algebra of a finite group. *Journal of Combinatorial Theory*, 2(4):603 – 615, 1967.
23. R. Stanley. *Enumerative Combinatorics*, volume 1. Cambridge University Press, second edition, 2011. <http://www-math.mit.edu/~rstan/ec/ec1/>.
24. P. Traxler. *Exponential Time Complexity of SAT and Related Problems*. PhD thesis, ETH Zürich, 2010.
25. R. Williams. Finding paths of length k in $\mathcal{O}^*(2^k)$ time. *Inf. Process. Lett.*, 109(6):315–318, 2009.
26. G. J. Woeginger. Open problems around exact algorithms. *Discrete Applied Mathematics*, 156(3):397–405, 2008.
27. F. Yates. *The design and analysis of factorial experiments*. Brasilia: EMBRAPA-DMQ, 1937.
28. R. Zippel. Probabilistic algorithms for sparse polynomials. In E. Ng, editor, *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer Berlin / Heidelberg, 1979.

APPENDIX

A Omitted proofs

A.1 Proofs omitted in Section 3

Proof of Corollary 7 For the proof we use the following result as a blackbox:

Theorem 19 ([16]) *Given an instance (\mathbf{a}, t) of SUBSET SUM, $c(\mathbf{a})_t$ can be computed in $\mathcal{O}^*(t)$ time and $\mathcal{O}^*(1)$ space.*

Proof (of Corollary 7). By reducing modulo p we can assume that $a_1, \dots, a_n, t < p$. We have

$$c^p(\mathbf{a})_t = \sum_{i \equiv t \pmod{p}}^n c(\mathbf{a})_i = \sum_{j=0}^n c(\mathbf{a})_{t+jp},$$

where the first equality holds by definition and the second equality follows from the fact that $c(\mathbf{a})_i = 0$ when $i > np$ or $0 < i$. The latter expression can be evaluated in the claimed resource bounds using Theorem 19. \square

Proof of Theorem 9 Take an integer $i \leq u$ uniformly at random, and check whether it is a prime using the polynomial time algorithm of [1]. If i is prime, then output i and halt; otherwise repeat. If no prime is found after $\ln(u) + 2$ repetitions, output **notfound** and halt. The upper bound on the probability of failure follows from Theorem 8 since the probability that **notfound** is returned is at most $(1 - (\ln(u) + 2)^{-1})^{\ln(u)+2} \leq \frac{1}{e}$.

Proof of Theorem 1(b)) Let $\beta = \lceil \log \max\{t, \max_i a_i\} \rceil$. Call a prime p *bad* if $c(\mathbf{a})_t \neq c^p(\mathbf{a})_t$. Analogously to the proof of Lemma 10, there are at most $(\beta + \lceil \log n \rceil)S$ bad primes. Let p_1, \dots, p_l be the first l prime numbers in increasing order where $l = 2(\beta + \lceil \log n \rceil)S + 1$. Since there are only $(\beta + \lceil \log n \rceil)S$ bad primes, the majority of the set of integers $\{c^{p_i}(\mathbf{a})_t\}_{1 \leq i \leq l}$ will be equal to $c(\mathbf{a})_t$. Then use the folklore Majority voting algorithm [5] as in Algorithm A.1:

The correctness follows from the above discussion and the correctness of the majority voting algorithm [5] that is folklore and implemented in the algorithm. For the running time, note that p_l is $\mathcal{O}^*(S)$ by Theorem 8 and hence the running time is $\mathcal{O}^*(S^2)$ since Step 6 takes time $\mathcal{O}^*(S)$. It is clear that the algorithm can be implemented using polynomial space.

A.2 Proofs omitted in Section 4

Proof of Claim 1 For every $\mathbf{a}, \mathbf{b} \in \mathbb{N}[\mathbb{Z}_2^n]$ we have $(\mathbf{a} + \mathbf{b})\mathbf{H} = \mathbf{a}\mathbf{H} + \mathbf{b}\mathbf{H}$ and hence h is easily seen to be a homomorphism by Observation 4. Thus, by Observation 6 we know that $\mathbf{w} = h(\mathbf{v})$, that is, for every $\mathbf{z} \in \mathbb{Z}_2^s$

$$\mathbf{w}_{\mathbf{z}} = \sum_{\mathbf{y} \in \mathbb{Z}_2^n : \mathbf{y}\mathbf{H} = \mathbf{z}} \mathbf{v}_{\mathbf{y}}.$$

```

1:  $M, C, i, j \leftarrow 0$ .
2: while  $i \leq l$  do
3:    $j \leftarrow j + 1$ 
4:   if the deterministic primality testing from [1] returns that  $j$  is prime then
5:      $i \leftarrow i + 1$ ;  $p_i \leftarrow j$ 
6:     Compute  $c^{p_i}(\mathbf{a})_t$  using Corollary 7.
7:     if  $M = 0$  then
8:        $C \leftarrow c^{p_i}(\mathbf{a})_t$ 
9:     else if  $c^{p_i}(\mathbf{a})_t = C$  then
10:       $M \leftarrow M + 1$ 
11:     else
12:       $M \leftarrow M - 1$ 
13: return  $C$ 

```

Hence, if $\mathbf{v}_t \neq \mathbf{w}_{tH}$, there must exist $\mathbf{y} \in \text{supp}(\mathbf{v})$ such that $\mathbf{y} \neq \mathbf{t}$ and $\mathbf{y}H = \mathbf{t}H$. Equivalently, $(\mathbf{y} - \mathbf{t})H = \mathbf{0}$. For any $\mathbf{x} \in \mathbb{Z}_2^s$ with $\mathbf{x} \neq \mathbf{0}$ we have

$$\text{Prob}_H[\mathbf{x}H = \mathbf{0}] = \prod_{i=1}^s \text{Prob}_H[(\mathbf{x}H)_i = 0] = 2^{-s},$$

where the probability is taken uniform over all binary $s \times n$ matrices, and the two equalities follow from the fact that the random variables $(\mathbf{x}H)_i$ for $i = 1, \dots, s$ are independent and uniformly distributed. Now the claim follows by taking the union bound over all elements in the support:

$$\text{Prob}[\mathbf{v}_t \neq \mathbf{w}_{tH}] \leq \text{Prob}[\exists \mathbf{x} \in \text{supp}(\mathbf{v}) : \mathbf{x} \neq \mathbf{t} \wedge \mathbf{x}H = \mathbf{t}H] \leq |S|2^{-s} \leq \frac{1}{2}.$$

Proof of Claim 2 Let $\mathbf{b} \in \mathbb{N}[\mathbb{Z}_2^s]$ such that $\mathbf{b}_x = \text{sub}(C_1, \mathbf{x})$ for every $\mathbf{x} \in \mathbb{Z}_2^s$. It suffices to show that $\mathbf{b} = \mathbf{w}\Phi$ since hashZ2 returns $\frac{1}{2^s}(\mathbf{b}\Phi)_{tH}$ as can be seen from Line 4, and this is equal to \mathbf{w}_{Ht} by Lemma 12. For proving that $\mathbf{b} = \mathbf{w}\Phi$, we first claim that φ is a homomorphism from $\mathbb{N}[\mathbb{Z}_2^s]$ to \mathbb{N} since, for $\mathbf{a}, \mathbf{b} \in \mathbb{N}[\mathbb{Z}_2^s]$, we have that $\varphi(\mathbf{a} + \mathbf{b})$ equals

$$\sum_{\mathbf{y} \in \mathbb{Z}_2^s} (-1)^{\mathbf{x}\mathbf{y}^T} (a_{\mathbf{y}} + b_{\mathbf{y}}) = \sum_{\mathbf{y} \in \mathbb{Z}_2^s} (-1)^{\mathbf{x}\mathbf{y}^T} a_{\mathbf{y}} + \sum_{\mathbf{y} \in \mathbb{Z}_2^s} (-1)^{\mathbf{x}\mathbf{y}^T} b_{\mathbf{y}} = \varphi(\mathbf{a}) + \varphi(\mathbf{b}),$$

and $\varphi(\mathbf{a} * \mathbf{b})$ equals

$$\sum_{\mathbf{y} \in \mathbb{Z}_2^s} (-1)^{\mathbf{x}\mathbf{y}^T} \sum_{\mathbf{y}_1 + \mathbf{y}_2 = \mathbf{y}} a_{\mathbf{y}_1} b_{\mathbf{y}_2} = \sum_{\mathbf{y}_1 \in \mathbb{Z}_2^s} (-1)^{\mathbf{x}\mathbf{y}_1^T} a_{\mathbf{y}_1} \sum_{\mathbf{y}_2 \in \mathbb{Z}_2^s} (-1)^{\mathbf{x}\mathbf{y}_2^T} b_{\mathbf{y}_2} = \varphi(\mathbf{a})\varphi(\mathbf{b}).$$

Then, by Observation 6, $\text{sub}(C_1, \mathbf{x})$ returns $\varphi(\mathbf{w})$. For $\mathbf{a} \in \mathbb{Z}[\mathbb{Z}_2^s]$ we have $\varphi(\mathbf{a}) = (\mathbf{a}\Phi)_x$ so $\text{sub}(C_1, \mathbf{x}) = (\mathbf{w}\Phi)_x$ and hence $\mathbf{b} = \mathbf{w}\Phi$.

Proof of Theorem 15

Proof (of Theorem 15.a)). Use Theorem 2. Assume $\mathcal{F} = \{S_1, \dots, S_n\}$ and create the instance $(\mathbf{A}, \mathbf{b}, \omega, t')$ of LINEAR SAT where \mathbf{A} is the incidence matrix of the set system (\mathcal{F}, U) , $\mathbf{b} = 1$, $\omega_i = |S_i|n + 1$ and $t' = nm + t$. It is easy to see that the algorithm of Theorem 2 returns exactly the number of set partitions of size at most t \square

For the second part we will need the following folklore result.

Theorem 20 (Fast Walsh-Hadamard transform, Folklore) *Given a vector $\mathbf{a} \in \mathbb{N}[\mathbb{Z}_2^s]$, $\mathbf{a}\Phi$ can be computed in time $\mathcal{O}(2^s s)$ and using $\mathcal{O}(2^s s)$ operations in \mathbb{N} .*

Proof (of Theorem 15.b)). Consider the following circuit C over $\mathbb{Q}[\mathbb{Z}_2^m]$:

$$f[i, j] = \begin{cases} \langle 1, \mathbf{0} \rangle & \text{if } i = j = 0 \\ 0 & \text{if } i = 0 \text{ and } j \neq 0 \\ \sum_{h=0}^j f[i-1, h]g[j-h] & \text{otherwise, where} \end{cases} \quad (3)$$

$$g[j] = \sum_{i=1}^n [|S_i| = j] \langle 1, S_i \rangle \quad (4)$$

For every $\mathbf{x} \in \mathbb{Z}_2^m$ and non-negative integers i and j , the coefficient $f[i, j]_{\mathbf{x}}$ counts the number of ways to choose an i -tuple of sets in \mathcal{S} such that their sizes sum up to j and their characteristic vectors sum to \mathbf{x} in \mathbb{Z}_2^m . Thus $\text{supp}(f[t, m]) \leq 2^{\text{rk}(\mathbf{A})}$. Furthermore, $f[t, m]_{\mathbf{1}}$ is the number of set partitions of size t times $t!$. Indeed, if a t -tuple of sets from \mathcal{S} contributes to $f[t, n]_{\mathbf{1}}$, each element of U must occur in a unique set in the t -tuple. It remains to compute $(f[t, n]_{\mathbf{1}})$. For this we will use algorithm `hashZ2` with $s = \text{rk}(A)$, except that we replace Line 4 with the following to compute \mathbf{w}_{tH} , where \mathbf{w} is the output of C_1 :

```

4: for every  $0 \leq j \leq m$  do
5:   Compute and store  $h(g[j])$  using (4)
6:   Compute and store  $h(g[j])\Phi$  using Theorem 20
7: return  $\frac{1}{2^s} \sum_{\mathbf{x} \in \mathbb{Z}_2^s} (-1)^{(\mathbf{1}H)\mathbf{x}^T} (\mathbf{w}\Phi)_{\mathbf{x}}$ , using (3) and the stored values to compute the
   vector  $\mathbf{w}\Phi$ .

```

Algorithm 2: Changes to Algorithm 1 to implement Theorem 15.

The correctness follows from Claim 1 and the observation that the inversion formula from Theorem 12 is returned on Line 7. Indeed, h is a homomorphism and Φ is a bijective homomorphism, so Observation 6 enables us to compute $\mathbf{w}\Phi$ using (4).

To establish the time and space complexity, we observe that Steps 5 and 6 take $(2^s + n)m^{\mathcal{O}(1)}$ time by elementary analysis and Theorem 20, and that

Step 7 takes $2^s m^{\mathcal{O}(1)}$ time since we can compute $\mathbf{w} = h(\mathbf{f}[t, m])$ via (3) in $\mathcal{O}(m^3)$ operations in $\mathbb{Q}^{\mathbb{Z}_s^2}$ by relying on the stored values $h(\mathbf{g}[j])\Phi$, where each operation requires $\mathcal{O}(2^s s)$ time by Theorem 20. \square

A.3 Proofs of Section 5

This section is dedicated to the proof of Theorem 16. Instead of a combinatorial proof similar to the one of Section 5, we use the algebraic perspective in this proof since we feel it gives a more fundamental insight into the hashing function used. To obtain Theorem 16, we prove the following generalization of Lemma 17.

Lemma 21 *There is an algorithm that, given circuit C over $\mathbb{N}[(2^U, \cup)]$ with singleton inputs outputting \mathbf{v} , and a set family $\mathcal{F} \subseteq 2^U$ such that $\text{supp}(\mathbf{v}) \subseteq \mathcal{F}$ computes a list with v_X for every $X \in \text{supp}(\mathbf{v})$ in $\mathcal{O}^*(|\mathcal{F}|^2)$ time.*

From Lemma 21 to Theorem 16. We now combine Lemma 21 with the iterative compression technique to obtain Theorem 16 in a way very similar to Section 5. Instead of the subformula ϕ_i from Section 5, we need the following notion.

Definition 22 *Given a circuit C over $\mathbb{N}[(2^U, \cup)]$ and $X \subseteq U$, the restriction of C to X is the circuit obtained by applying the function h to it, where, for $Y \subseteq X$*

$$h(\mathbf{v})_Y = \sum_{W \subseteq U: W \cap X = Y} v_W.$$

Proof (of Theorem 16). Assume $U = \{e_1, e_2, \dots, e_n\}$, and for every $i = 0, \dots, n-1$, let C^i be the restriction of C to $\{e_1, \dots, e_i\}$ and \mathbf{v}^i be the output of C^i . Then, since taking restrictions is homomorphic, we have by Observation 6 that

$$v_Y^i = \sum_{W \subseteq U: W \cap \{e_1, \dots, e_i\} = Y} v_W \leq \sum_{W \subseteq U: W \cap \{e_1, \dots, e_{i-1}\} = Y \setminus \{e_i\}} v_W = v_{Y \setminus \{e_i\}}^{i-1}.$$

This implies that if $X \in \text{supp}(\mathbf{v}^i)$, then $X \setminus \{e_i\} \in \text{supp}(\mathbf{v}^{i-1})$ and hence

$$\text{supp}(\mathbf{v}^i) \subseteq \text{supp}(\mathbf{v}^{i-1}) \cup \{X \cup \{e_i\} : X \in \text{supp}(\mathbf{v}^{i-1})\}. \quad (5)$$

We now describe how to implement the theorem. First note that $\text{supp}(\mathbf{v}^0) = \emptyset$. For $i = 1, \dots, n$ do the following: set $\mathcal{F}^i = \text{supp}(\mathbf{v}^{i-1}) \cup \{X \cup \{e_i\} : X \in \text{supp}(\mathbf{v}^{i-1})\}$. Then by (5), $\text{supp}(\mathbf{v}^i) \subseteq \mathcal{F}^i$. Hence, by invoking the algorithm of Lemma 21 using C^i as the circuit and \mathcal{F}^i as the set family, we can obtain v_X^i for every $X \in \text{supp}(\mathbf{v}^i)$ in $\mathcal{O}^*(|\mathcal{F}^i|^2)$ time which is $\mathcal{O}^*((2|\text{supp}(\mathbf{v}^{i-1})|)^2)$ time. From these values we can easily obtain the support of \mathbf{v}^i . After n steps, we have computed $v_X = v_X^n$ for every $X \in \text{supp}(\mathbf{v})$. The claimed running time follows from the fact that $|\text{supp}(\mathbf{v}^{i-1})| \leq |\text{supp}(\mathbf{v}^i)|$ for every $i = 1, \dots, n$. \square

The remainder of this section is devoted to the proof of Lemma 21. The idea is to use the set family \mathcal{F} to create a poset and homomorphically hash $\mathbb{N}[(2^U, \cup)]$ to the so-called Solomon algebra of the poset. We will first recall all necessary notions and properties, second introduce the hash function, and third give the algorithm implementing Lemma 21.

Preliminaries on Möbius inversion and the Solomon algebra Let (P, \leq) be a poset. An element $c \in P$ is said to be an *upper bound* of a set $X \subseteq P$ if $x \leq c$ holds for all $x \in X$. The set X is said to have a *join* in P if there exists an upper bound $c \in P$ (called *the join*) of X such that, for all upper bounds d of X , it holds that $c \leq d$. For $X \subseteq P$, let us write $\bigvee X$ for the join of X ; for the join of $X = \{a, b\}$ we write simply $a \vee b$. The *open interval* (x, y) is the poset induced by the set $\{e \in P : x < e < y\} \subseteq P$. We write $[x, y)$, $(x, y]$ and $[x, y]$ for the analogous (half-)closed interval.

Let P be a poset. The *Möbius function* $\mu : P \times P \rightarrow \mathbb{N}$ of P is defined for all $x, y \in P$ by

$$\mu(x, y) = \begin{cases} 1 & \text{if } x = y, \\ -\sum_{x \leq z < y} \mu(x, z) & \text{if } x < y, \\ 0 & \text{otherwise.} \end{cases} \quad (6)$$

The *zeta transform* ζ and *Möbius transform* μ are the $|P| \times |P|$ matrices defined by $\zeta_{x,y} = [x \leq y]$ and $\mu_{x,y} = \mu(x, y)$ for all $x, y \in P$.

The following combinatorial interpretation is particularly useful:

Theorem 23 (Hall (see [23], Proposition 3.8.5)) *For all $x, y \in P$, $\mu(x, y)$ is the number of even chains in (x, y) minus the number of odd chains in (x, y) .*

We include a proof for completeness

Proof. Use induction on the number of elements in the interval (x, y) . If $x = y$, (x, y) contains only the empty chain, which is even. If $x < y$, group all chains on their smallest element y . The contribution of all these chains is exactly $-\mu(y, z)$ since odd chains are extended to even chains and vice-versa by adding y . \square

It is known that μ and ζ are mutual inverses. To see this, note that $(\mu\zeta)_{xy}$ can be interpreted as the number of even chains minus the number of odd chains in the interval $(x, y]$ which can be seen to be 0 if $x \neq y$ by a pairing argument, and 1 otherwise. This principle is called *Möbius inversion*.

Definition 24 ([22]) *Let (P, \leq) be a poset. The Solomon algebra $\mathbb{N}[P]$ is the set \mathbb{N}^P equipped with coordinate-wise addition \oplus and the Solomon product \otimes defined for all $\mathbf{f}, \mathbf{g} \in \mathbb{N}[P]$ and $z \in P$ by*

$$(\mathbf{f} \oplus \mathbf{g})_z = f_z + g_z \quad (\mathbf{f} \otimes \mathbf{g})_z = \sum_{x, y \in P} \left(\sum_{x, y \leq q \leq z} \mu(q, z) \right) f_x g_y$$

The following properties of the Solomon algebra will be useful:

Lemma 25 *For every $\mathbf{v}^1, \dots, \mathbf{v}^k \in \mathbb{N}[P]$ and $s \in P$ we have*

$$\left(\bigotimes_{i=1}^n \mathbf{v}^i \right)_s = \sum_{a_1, \dots, a_k \in P} \left(\sum_{a_1, \dots, a_k \leq r \leq s} \mu(r, s) \right) \prod_{i=1}^k v_{a_i}^i$$

Proof. Use induction of n . For $n = 1$, the statement clearly holds. Otherwise, we have by definition of \otimes that

$$\begin{aligned}
\left(\bigotimes_{i=1}^k v^i \right)_s &= \sum_{w, a_k \in P} \left(\sum_{w, a_k \leq r \leq s} \mu(r, s) \right) \left(\bigotimes_{i=1}^{k-1} v^i \right)_w v_{a_k}^k \\
&\quad \{\text{Induction Hypothesis}\} \\
&= \sum_{w, a_k \in P} \left(\sum_{w, a_k \leq r \leq s} \mu(r, s) \right) \sum_{a_1, \dots, a_{k-1} \in P} \left(\sum_{a_1, \dots, a_{k-1} \leq q \leq w} \mu(q, w) \right) \prod_{i=1}^k v_{a_i}^i \\
&\quad \{\text{Reordering summations}\} \\
&= \sum_{a_1, \dots, a_k, w \in P} \left(\sum_{\substack{w, a_k \leq r \leq s \\ a_1, \dots, a_{k-1} \leq q \leq w}} \mu(r, s) \mu(q, w) \right) \prod_{i=1}^k v_{a_i}^i \\
&\quad \{\text{Reordering summations}\} \\
&= \sum_{a_1, \dots, a_k \in P} \sum_{\substack{a_1, \dots, a_{k-1} \leq q \\ a_k \leq r}} \left(\sum_{q \leq w \leq r} \mu(q, w) \right) \mu(r, s) \prod_{i=1}^k v_{a_i}^i \\
&\quad \{\text{Möbius inversion}\} \\
&= \sum_{a_1, \dots, a_k \in P} \sum_{\substack{a_1, \dots, a_{k-1} \leq q \\ a_k \leq r}} [q = r] \mu(r, s) \prod_{i=1}^k v_{a_i}^i \\
&= \sum_{a_1, \dots, a_k \in P} \left(\sum_{a_1, \dots, a_k \leq q} \mu(q, s) \right) \prod_{i=1}^k v_{a_i}^i
\end{aligned}$$

□

Theorem 26 ([22]) *The zeta transform is a homomorphism from $\mathbb{N}[P]$ to \mathbb{N}^P ; that is, for every $\mathbf{f}, \mathbf{g} \in \mathbb{N}[P]$ it holds that $(\mathbf{f} \oplus \mathbf{g})\zeta = \mathbf{f}\zeta + \mathbf{g}\zeta$ and $(\mathbf{f} \otimes \mathbf{g})\zeta = \mathbf{f}\zeta \circ \mathbf{g}\zeta$.*

Proof. For every $w \in P$ we have

$$\begin{aligned}
((\mathbf{f} \oplus \mathbf{g})\zeta)_w &= \sum_{z \leq w} (f_z + g_z) = \sum_{z \leq w} f_z + \sum_{z \leq w} g_z = (\mathbf{f}\zeta)_w + (\mathbf{g}\zeta)_w, \quad \text{and} \\
((\mathbf{f} \otimes \mathbf{g})\zeta)_w &= \sum_{z \leq w} \sum_{x, y \in P} \left(\sum_{x, y \leq q \leq z} \mu(q, z) \right) f_x g_y \\
&= \sum_{x, y, q, z \in P} [x, y \leq q \leq z \leq w] \mu(q, z) f_x g_y \\
&= \sum_{x, y, q \in P} [x, y \leq q \leq w] \left(\sum_{q \leq z \leq w} \mu(q, z) \right) f_x g_y \\
&= \sum_{x, y, q \in P} [x, y \leq q \leq w] [q = w] f_x g_y \\
&= \sum_{x, y \in P} [x, y \leq w] f_x g_y = \left(\sum_{x \leq w} f_x \right) \left(\sum_{y \leq w} g_y \right) = (\mathbf{f}\zeta)_w (\mathbf{g}\zeta)_w.
\end{aligned}$$

□

Lemma 27 ([22]) *Let P be a poset with a minimum element $\hat{0}$. Then, $\mathbb{N}[P]$ is a commutative ring with the multiplicative identity $\langle 1, \hat{0} \rangle$.*

Proof. The singleton $\langle 1, \hat{0} \rangle$ is the multiplicative identity because

$$(\langle 1, \hat{0} \rangle \otimes \mathbf{g})_z = \sum_{y \leq z} \left(\sum_{y \leq q \leq z} \mu(q, z) \right) g_y = g_z,$$

where the last equality follows from Möbius inversion. To see that $\mathbb{N}[P]$ is a commutative ring, note that ζ is an isomorphism from $\mathbb{N}[P]$ to the ring \mathbb{N}^P . Indeed, Theorem 26 shows that ζ is a homomorphism, and $\zeta\mu = \mu\zeta = \mathbf{I}$ shows that ζ is bijective. □

Lemma 28 *For singletons $\langle c, x \rangle, \langle d, x \rangle \in \mathbb{N}[P]$ it holds that $\langle c, x \rangle \otimes \langle d, x \rangle = \langle cd, x \rangle$.*

Proof. For all $z \in P$, we have that $(\langle c, x \rangle \otimes \langle d, x \rangle)_z$ equals

$$\sum_{w, y \in P} \left(\sum_{w, y \leq q \leq z} \mu(q, z) \right) [w = x]c[y = x]d = \sum_{x \leq q \leq z} \mu(q, z)cd = [x = z]cd.$$

□

The hash function for Lemma 21 Let U be an n -element set and let (P, \leq) be a poset that satisfies $U \subseteq P$ and has a minimum element $\hat{0}$. Define the function $h : \mathbb{N}[(2^U, \cup)] \rightarrow \mathbb{N}[P]$ by setting, for all $\mathbf{a} \in \mathbb{N}[(2^U, \cup)]$,

$$h(\mathbf{a}) = \bigoplus_{X \subseteq U} \langle a_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle. \quad (7)$$

The following two lemmas combined show that the function h is in fact an homomorphic hash function:

Lemma 29 *If (P, \leq) is a poset with minimum element, $U \subseteq P$ and $\mathbf{v} \in \mathbb{N}[(2^U, \cup)]$ such that every $X \in \text{supp}(\mathbf{v})$ has a join in P and for every $X, Y \in \text{supp}(\mathbf{v})$,*

$$\vee \{\{e\} : e \in X\} \neq \vee \{\{e\} : e \in Y\}, \quad (8)$$

then for every $X \in \text{supp}(\mathbf{v})$, $h(\mathbf{v})_{\vee \{\{e\} : e \in X\}} = v_X$.

Proof. Denote $y = \vee \{\{e\} : e \in X\}$. Then,

$$\begin{aligned} (h(\mathbf{v}))_y &= \left(\bigoplus_{X \subseteq U} \langle v_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right)_y \\ &\quad \{\text{for } X \notin \text{supp}(\mathbf{v}) \text{ we have } v_X = 0\} \\ &= \left(\bigoplus_{X \in \text{supp}(\mathbf{v})} \langle v_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right)_y \\ &\quad \{\text{Definition of } \oplus\} \\ &= \sum_{X \in \text{supp}(\mathbf{v})} \left(\langle v_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right)_y \\ &\quad \{\text{Applying Lemma 25, denoting } X = \{e_1, \dots, e_{|X|}\}\} \\ &= \sum_{X \in \text{supp}(\mathbf{v})} \sum_{a_0, \dots, a_{|X|} \in P} \left(\sum_{a_0, \dots, a_{|X|} \leq q \leq y} \mu(q, y) \right) v_X[a_0 = \hat{0}] \prod_{i=1}^{|X|} [a_i = e_i] \\ &\quad \{X \text{ has a join by assumption since it is in the support}\} \\ &= \sum_{X \in \text{supp}(\mathbf{v})} \left(\sum_{e_1 \vee \dots \vee e_{|X|} \leq q \leq y} \mu(q, y) \right) v_X \\ &\quad \{\text{Möbius inversion}\} \\ &= \sum_{X \in \text{supp}(\mathbf{v})} [e_1 \vee \dots \vee e_{|X|} = y] v_X \\ &\quad \{\text{By the assumption stated in (8)}\} \\ &= v_X \end{aligned}$$

□

Lemma 30 *The mapping h is a homomorphism from $\mathbb{N}[(2^U, \cup)]$ to $\mathbb{N}[P]$.*

Proof. For every $\mathbf{v}, \mathbf{w} \in \mathbb{Z}[(2^U, \cup)]$ we have

$$\begin{aligned}
h(\mathbf{v} + \mathbf{w}) &= \bigoplus_{X \subseteq U} \langle v_X + w_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \\
&= \bigoplus_{X \subseteq U} (\langle v_X, \hat{0} \rangle \oplus \langle w_X, \hat{0} \rangle) \otimes \bigotimes_{e \in X} \langle 1, e \rangle \\
&= \bigoplus_{X \subseteq U} \left(\langle v_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \oplus \langle w_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right) \\
&= \left(\bigoplus_{X \subseteq U} \langle v_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right) \oplus \left(\bigoplus_{X \subseteq U} \langle w_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right) \\
&= h(\mathbf{v}) \oplus h(\mathbf{w}).
\end{aligned}$$

$$\begin{aligned}
h(\mathbf{v} * \mathbf{w}) &= \bigoplus_{X \subseteq U} \langle (v * w)_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \\
&\quad \{ \text{Definition of multiplication in } \mathbb{N}[(2^U, \cup)] \} \\
&= \bigoplus_{X \subseteq U} \left\langle \sum_{V \cup W = X} v_V w_W, \hat{0} \right\rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \\
&\quad \{ \text{By definition of } \oplus \} \\
&= \bigoplus_{X \subseteq U} \bigoplus_{V \cup W = X} \langle v_V w_W, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \\
&\quad \{ \text{By Lemma 28 and commutativity of } \otimes \text{ from Lemma 27} \} \\
&= \bigoplus_{X \subseteq U} \bigoplus_{V \cup W = X} \langle v_V w_W, \hat{0} \rangle \otimes \bigotimes_{e \in V} \langle 1, e \rangle \otimes \bigotimes_{e \in W} \langle 1, e \rangle \\
&\quad \{ \text{Using that } V \text{ and } W \text{ determine } X \} \\
&= \bigoplus_{V, W \subseteq U} \langle v_V w_W, \hat{0} \rangle \otimes \bigotimes_{e \in V} \langle 1, e \rangle \otimes \bigotimes_{e \in W} \langle 1, e \rangle \\
&\quad \{ \text{By Lemma 28} \} \\
&= \bigoplus_{V, W \subseteq U} (\langle v_V, \hat{0} \rangle \otimes \langle w_W, \hat{0} \rangle) \otimes \bigotimes_{e \in V} \langle 1, e \rangle \otimes \bigotimes_{e \in W} \langle 1, e \rangle \\
&\quad \{ \text{By distributivity from Lemma 27} \} \\
&= \left(\bigoplus_{X \subseteq U} \langle v_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right) \otimes \left(\bigoplus_{X \subseteq U} \langle w_X, \hat{0} \rangle \otimes \bigotimes_{e \in X} \langle 1, e \rangle \right) \\
&= h(\mathbf{v}) \otimes h(\mathbf{w}).
\end{aligned}$$

□

The algorithm for Lemma 21 We are now ready to give the proof of Lemma 21. As mentioned before, the proof idea is to construct a poset P from the given set family and hash the given circuit to a circuit C' over the Solomon algebra $\mathbb{N}[P]$ with the homomorphic hash function h . Then by Theorem 26 and Lemma 30, the zeta-transform of the output of C' can be computed fast using point-wise multiplication, and then using Möbius inversion the original output can be computed. Because of the hash property from Lemma 29 of h , the required output of C can then be read from the output of C' .

Proof (of Lemma 21). We start by giving the algorithm. We assume without loss of generality that $\emptyset \in \mathcal{F}$.

Algorithm find(C, \mathcal{F})

- 1: Construct the poset $P = (\mathcal{F}, \subseteq)$.
- 2: Construct the circuit C_1 over $\mathbb{N}[P]$ obtained from C by applying h .
- 3: **for** every $x \in P$ **do**
- 4: $w_x \leftarrow \text{sub}(C_1, x)$.
- 5: **return** $\text{mobius}(P, w)$

Algorithm sub(C_1, x)

- 6: Construct the circuit C_2 over \mathbb{N} obtained from C_1 by applying $\zeta_x : e \mapsto \sum_{y \leq x} e_y$.
- 7: Evaluate C_2 and return the output.

Algorithm mobius($(P, \leq), w$)

- 8: Let $P = \{v_1, v_2, \dots, v_{|P|}\}$ such that $v_i \leq v_j$ implies $i \geq j$.
- 9: $z \leftarrow w$.
- 10: **for** $i = 1, 2, \dots, |P|$ **do**
- 11: **for** every $v_j \leq v_i$ **do**
- 12: $z_i = z_i - z_j$
- 13: **return** z .

The algorithm is Algorithm **find**. Let us first analyse the complexity. Recall that to establish the claimed bounds we assume that each operation in \mathbb{N} takes one time unit. Step 1 can easily be implemented in $\mathcal{O}(|\mathcal{F}|)$ time. Step 2 expands every singleton (of $\mathbb{N}[(2^U, \cup)]$) in C according to (7) into a product of at most $n + 1$ singletons of $\mathbb{N}[P]$, and thus can be implemented in time and storage $\mathcal{O}(n|C|)$. Step 6 can be implemented in time and space $\mathcal{O}(|C_1|)$ because the singleton $e = \langle v, y \rangle$ is mapped to $[y \leq x]v$. In Step 7, the evaluation of C_2 over \mathbb{N} uses $|C_2|$ operations in \mathbb{N} . The complexity of algorithm **mobius** is easily seen to be $\mathcal{O}^*(|\mathcal{F}|^2)$, and since the loop at Step 3 is the only other time-consuming part the resource bounds are clearly met.

We proceed with the proof of correctness of Algorithm **find**. First note that since $\text{supp}(w) \subseteq \mathcal{F}$, we have by construction that for every $X = \{e_1, \dots, e_{|X|}\} \in \text{supp}(w)$, $\vee\{\{e_1\}, \dots, \{e_{|X|}\}\} = X$, since every other upper bound in P on $\{\{e_1\}, \dots, \{e_{|X|}\}\}$ must be above the element X of P . This directly implies that the requirement imposed by (8) is met by P . Hence by Lemma 29 we have

that $h(\mathbf{v})_{\vee\{\{e\}:e\in X\}} = v_X$ for every $X \in \text{supp}(\mathbf{v})$. Thus to prove correctness it suffices to show that the vector $\mathbf{w}\boldsymbol{\zeta}$ is equal to $h(\mathbf{v})$.

Since h is a homomorphism by Lemma 30, Observation 6 implies that C^1 outputs $h(\mathbf{v})$. Then, we claim that for every $x \in P$ it holds that $w_x = \text{sub}(C_1, x) = (h(\mathbf{v})\boldsymbol{\zeta})_x$. To see this note that on Line 7 first the zeta transform is applied to C_1 which is a homomorphism to \mathbb{N}^P by Theorem 26, and then we restrict to the coordinate x . The claim then follows by Observation 6 since both transformations are homomorphisms.

Finally, since $w_x = (h(\mathbf{v})\boldsymbol{\zeta})_x$, we know that $(\mathbf{w}\boldsymbol{\mu}) = h(\mathbf{v})$. The lemma then follows since it is easy to see that $\text{mobius}(P, \mathbf{w}) = \mathbf{w}\boldsymbol{\mu}$. \square

Proof of Theorem 16(b) The proof of Item (b) is fairly similar to the proof of Item (a). The main difference is the use of the poset P . In this section, we will use a poset larger than the support of \mathbf{v} , but the advantages are that

1. we not need to construct the poset using Iterative compression, and hence we do not need to determine all components of \mathbf{v} ,
2. the poset will be decomposable, implying that the bottleneck in (a), the Möbius inversion step, can be improved.

Let us now start with the more formal treatment. Given two posets (P, \leq_P) and (Q, \leq_Q) , the *direct product* $P \times Q$ is the poset on the set $\{(p, q) : p \in P \wedge q \in Q\}$ such that $(p_1, q_1) \leq (p_2, q_2)$ if $p_1 \leq_P p_2$ and $q_1 \leq_Q q_2$.

Lemma 31 (see [23], **Proposition 3.8.2**) *Let P and Q be posets and let μ_P and μ_Q denote their respective Möbius functions. Denote $\mu_{P \times Q}$ and \leq for the Möbius function and order of $P \times Q$, then for $(p_1, q_1) \leq (p_2, q_2)$ it holds that*

$$\mu_{P \times Q}((p_1, q_1), (p_2, q_2)) = \mu_P(p_1, p_2) \mu_Q(q_1, q_2).$$

Lemma 32 ([27], “Yates’ algorithm”) *Given a vector $\mathbf{v} \in \mathbb{N}^{2^U}$, there is an algorithm that computes the vector $\mathbf{v}\boldsymbol{\mu}$ in $\mathcal{O}(2^{|U|}|U|)$ time.*

We will also need the following small modification of Yates’ algorithm:

Lemma 33 *There is an algorithm that, given a poset $P \subseteq 2^U$ ordered by set inclusion and containing \emptyset and U , computes a table with $\mu(0, S)$ and $\mu(S, U)$ for every $S \in P$ in $\mathcal{O}(|P| \cdot |U|)$ time and space*

Proof. In this proof $[i]$ denotes the set $\{1, \dots, i\}$ for an integer i . Let $U = [n]$. We first define $g : [n] \rightarrow \mathbb{N}$ by letting

$$g(S) = \begin{cases} 1 & \text{if } S = \emptyset, \\ \sum_{\substack{Y \in P \\ Y \subset S}} -g(Y) & \text{otherwise.} \end{cases}$$

It is easy to see that $g(S) = \mu(\emptyset, S)$. Also, define for every $i = 1, \dots, n$:

$$f_i(S) = \begin{cases} 1 & \text{if } i = 0 \text{ and } S = \emptyset \\ -[S \in P]g(S) & \text{if } i = 0 \text{ and } S \neq \emptyset \\ f_{i-1}(S) + [i \in S]f_{i-1}(S \setminus i) & \text{otherwise.} \end{cases}$$

Then it holds that $g(S) = f_n(S)$ for every $S \subseteq U$. Note that by symmetry (that is, reversing the order of the poset), this procedure can be used as well to compute $\mu(S, U)$ for every $S \in P$ in the same time bounds. \square

Lemma 34 *There is an algorithm that, given an integer s and a circuit C with singleton inputs in $\mathbb{N}[(2^U, \cup)]$ outputting \mathbf{v} , computes v_U in time*

$$\mathcal{O}^*(\max\{2^s, |\text{supp}(\phi_s)|2^{n-s}n^{\mathcal{O}(1)}\}).$$

Proof. Assume $U = \{e_1, e_2, \dots, e_n\}$, and let C^s be the restriction of C to $U_s = \{e_1, \dots, e_s\}$ and \mathbf{v}^s be the output of C^s .

Claim 3 *There is an algorithm computing $\text{supp}(\mathbf{v}^s)$ in $\mathcal{O}^*(2^s n^{\mathcal{O}(1)})$ time.*

Proof. By Theorem 26, ζ is a homomorphism from $\mathbb{N}[P]$ to \mathbb{N}^P . Hence, similarly as in the proof of Theorem 16(a), we can compute $\mathbf{v}^s \zeta$ in time polynomial in the input size. Then the claim follows directly by applying Lemma 32. \square

Now the algorithm is as follows

Algorithm find2(C)

- 1: Obtain $\text{supp}(\mathbf{v}^s)$ using Claim 3
- 2: Let $P' = (\text{supp}(\mathbf{v}^s), \subseteq)$ and $Q = (2^{U \setminus U_s}, \subseteq)$ and construct the poset $P = P' \times Q$.
- 3: Construct the circuit C_1 over $\mathbb{N}[P]$ obtained from C by applying the homomorphism h as defined in (7).
- 4: **for** every $x \in P$ **do**
- 5: $w_x \leftarrow \text{sub}(C_1, x)$.
- 6: Compute $\mu(0, x)$ for every $x \in P'$ using Lemma 33.
- 7: **return** $\sum_{x=(X_1, X_2) \in P} w_x \mu(X_1, U_s) (-1)^{|(U \setminus U_s) \setminus X_2|}$

The arguments for the correctness of this algorithm are all similar to the arguments of for the correctness of Algorithm **find2**: first note that $\text{supp}(v) \subseteq \{X_1 \cup X_2 : X_1 \in P' \wedge X_2 \in Q\}$. This in turn implies the condition of Lemma 29, and hence if \mathbf{v}' is the output of C^1 we indeed have that $v'_U = v_U$. As shown before in the proof of Lemma 21, $\text{sub}(C_1, x) = (\mathbf{v}' \zeta)_x$. Hence it remains the show that on Line 7 the expression is indeed the Möbius inversion formula. This follows from the definition of μ , the direct product property of the Möbius function from Lemma 31 and the fact that in the subset lattice $\mu(X, Y) = (-1)^{|Y \setminus X|}$ for $X \subseteq Y$.

For the running time of the above algorithm, note that Line 1 takes $\mathcal{O}^*(2^s n^{\mathcal{O}(1)})$ time. For Line 2, we have $|P'| \leq |\text{supp}(\mathbf{v})|$ and $|Q| = 2^{n-s}$, and hence $|P| \leq |\text{supp}(\mathbf{v})|2^{n-s}$. Thus, Lines 2-5 take $\mathcal{O}^*(|\text{supp}(\mathbf{v})|2^{n-s} n^{\mathcal{O}(1)})$ time. Line 6 takes $\mathcal{O}^*(2^s n^{\mathcal{O}(1)})$ time, and using these values, Line 7 can be performed in time at most $\mathcal{O}^*(|\text{supp}(\mathbf{v})|2^{n-s} n^{\mathcal{O}(1)})$. \square

Given Lemma 33, the only thing left to prove Theorem 16(b) is to solve the technical issue that α is not given:

Proof (of Theorem 16(b)). Simultaneously try all integers $0 < s \leq n/2$, and for every s run the algorithm of Lemma 34. Terminate whenever any of these algorithms terminates. This procedure runs in time

$$\mathcal{O}^*\left(\min_{0 < s \leq n/2} \max\{2^s, |\text{supp}(\phi_s)|2^{n-s} n^{\mathcal{O}(1)}\}\right) \leq \mathcal{O}^*(2^{(1-\alpha/2)n}),$$

where the inequality is achieved by taking $s = \lfloor (1 - \alpha/2)n \rfloor$. \square